UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1–100, Defendants.	No. 2:17-cv-01880 COMPLAINT

I. INTRODUCTION

1. Defendants are engaged in a complex internet "phishing" scheme to unlawfully obtain account access credentials from Microsoft customers. Specifically, Defendants transmit misleading and deceptive "Account Update" emails to Microsoft customers in an effort to fraudulently obtain user names and passcodes for customers' Microsoft Accounts ("MSAs"). These emails falsely claim to be from Microsoft and direct the customers to a fake "Microsoft Office" login page. Customers attempting to access and update their account on the phony login page are at risk of their account information of being unlawfully captured and exploited by Defendants. Microsoft files this lawsuit to protect its customers and stop Defendants' cybercrime scheme.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

II. BACKGROUND

2. Phishing attacks are a serious and growing form of cybercrime that threatens millions of people in nearly every community across the planet. Cybercriminals target unsuspecting victims through spoofed emails purporting to be from legitimate entities or individuals. These emails are designed to and, in fact, often do trick people into divulging personal information, such as account credentials and credit card information. In addition to identity theft, phishing attacks can also expose innocent people to other harms, such as malicious software. Microsoft goes to great lengths to protect people from such attacks. Microsoft's efforts to stop phishing attacks start with engineering safeguards into its products. For example, Microsoft's Office 365 product contains sophisticated tools to stop these attacks from even reaching users. While Microsoft's safeguards prevent many different types of phishing attacks, some users are nevertheless tricked into divulging their sensitive information. Microsoft investigates the cybercriminals behind phishing attacks and takes enforcement actions, such as this one, to stop them.

III. PARTIES

3. Microsoft is a Washington corporation with its principal place of business in Redmond, Washington. Microsoft develops, markets, distributes, and licenses computer software, among other products and services.

4. The true identities of Defendants are presently unknown to Microsoft. On information and belief, Defendants designed, created, maintained, operated, and facilitated domains defendworld.eu and azure1.us in furtherance of a scheme to defraud Microsoft's customers by (among other things) unlawfully gaining access to Microsoft Office 365 accounts and other sensitive information as alleged in this Complaint.

IV. JURISDICTION & VENUE

5. The Court has original subject matter jurisdiction over Microsoft's federal claims pursuant to 15 U.S.C. § 1121 and 28 U.S.C. §§ 1331 and 1338(a). This Court has subject matter jurisdiction over Microsoft's state claim pursuant to 28 U.S.C. § 1367(a) because

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

it is so related to the federal claims in this action within the Court's original jurisdiction that they form part of the same case or controversy.

6. The Court has personal jurisdiction over Defendants because they purposefully directed their unlawful activities at Washington, and Microsoft's claims arise from those activities. Defendants expressly aimed their conduct at Washington because they (1) had actual or constructive knowledge of Microsoft's intellectual property rights (including Microsoft's registered trademarks) and Microsoft's residence in Washington where it controls its exclusive rights in its trademarks; (2) acted, at a minimum, with willful blindness to, or in reckless disregard of, Microsoft's rights, and in reckless disregard of the likelihood that it was infringing Microsoft's trademarks; and (3) knew or should have known that their conduct would cause harm to Microsoft in Washington because it is foreseeable that infringement of Microsoft's rights would cause harm likely to be suffered in Washington, the state of its residence, incorporation, and headquarters. *See Wash. Shoe Co. v. A-Z Sporting Goods, Inc.*, 704 F.3d 668 (9th Cir. 2012).

7. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the claims occurred in the Western District of Washington.

8. Pursuant to Local Civil Rule 3(d), intra-district assignment to the Seattle Division is proper because the claims arose in this Division, where (a) Microsoft resides, (b) the injuries giving rise to suit occurred, and (c) Defendants directed their unlawful conduct.

V. FACTS

A. Microsoft and Office 365

9. Office 365 signifies a revolutionary change in the way that Microsoft delivers its industry-leading software to consumers. Previously, Microsoft licensed its popular Office suite of productivity products—which includes Word, Excel, PowerPoint, Outlook, OneNote, Publisher, and Access, among others—to computer users who installed and stored the software on their computer systems locally.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

10. With Office 365, Microsoft Office is available on a subscription basis that uses and leverages Microsoft's Azure cloud technology. Now, customers purchase a subscription to Office 365 that provides access to both cloud and locally-stored versions of the software. This allows customers to receive instant access to the latest versions of each program, and use the programs across multiple devices (such as laptops, phones, tablets, etc.). An Office 365 subscription also comes with cloud storage.

11. Microsoft has duly and properly registered a number of trademarks in the United States Patent and Trademark Office on the Principal Register, including without limitation:

a. "MICROSOFT," Trademark and Service Mark Registration No. 1,200,236;

b. "Microsoft (Stylized) and Design 2012," Trademark and Service Mark Registration No. 4,552,363;

c. "Microsoft Design (Color) 2012," Trademark and Service Mark Registration No. 4,560,827;

d. "Office 365," Trademark and Service Mark Registration No. 4,185,310;

e. "Office 2012 Design," Trademark and Service Mark Registration No. 4,459,826;

f. "Office (w/ Office 2012 Design)," Trademark Registration No. 4,456,462;

g. "WINDOWS," Trademark Registration No. 1,872,264; and

h. "Windows Flag Design (2012)," Trademark Registration No. 4,400,958.

i. "Azure," Trademark and Service Mark Registration No. 4,932,997.

Microsoft has developed these trademarks and service marks and advertises, markets, distributes, and licenses products using them, including Office 365.

12. Office 365 can be licensed for consumer or personal use (through the Personal, Home or Student products) or for commercial use (through the Business or Enterprise products). Using either type of Office 365 service requires the establishment of online

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

accounts.

13. For the consumer use products, a user must create or use an existing MSA consisting of an email address and password.

14. The commercial Office 365 products are created for organizations, which are identified as Tenants. User accounts within a Tenant are set-up in one of two ways that take advantage of Microsoft's Azure Active Directory product—a cloud-based directory and identity management system. First, the Administrator of the Tenant can set up individual Office 365 Commercial User Accounts. Second, the Administrator can create several Accounts in bulk.

15. Microsoft is committed to protecting customers' MSAs, Tenants and Commercial User Accounts from unauthorized access, and has devoted tremendous financial and other resources to secure customer data.

B. The Global Threat from Phishing Attacks

16. Phishing is a broad term that can encompass many different activities. The most well-known phishing schemes fall under the umbrella of social engineering attacks. Generally, these schemes involve an individual or group creating spoofed emails that purport to be from legitimate businesses, agencies or individuals.

17. The initial emails can contain malicious files, but more commonly, these emails are designed to lead the recipient to fake websites that trick users into divulging sensitive information, such as financial account data, login credentials and other personally identifiable information. Criminals behind the fake websites harvest personal information and use it to access peoples' accounts for their own illicit gain. They also sell the personal information to other criminals who use it to inflict further harm on the victims.

18. Beyond stealing peoples' account credentials, the criminals behind these schemes may also use the initial email or fake website to infect users' computers with dangerous malware. This malware further exposes unsuspecting victims' personal information, for example, by searching the computer for sensitive files, or even monitoring key strokes to

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

harvest personally identifiable information entered into other websites. Malicious software also allows the criminals to hijack a computer or network to propagate further attacks.

19. Over the last several years, phishing attacks have become both more prevalent and more sophisticated. The Anti-Phishing Working Group ("APWG"), a nonprofit that works to stop phishing, reports that phishing attacks increased over 65% between 2015 and 2016 alone. *See* http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf. In fact, the APWG reports that phishing attacks have increased by a staggering 5,753% since 2004. There are tens of thousands of phishing sites that work to impersonate hundreds of brands. Phishing attacks have been blamed for a number of the most notorious recent cybersecurity incidents.

C. Microsoft's Efforts to Screen and Stop Malicious Attacks on Office 365 Users

20. One of the most effective ways to stop phishing schemes is to prevent the harmful messages from even reaching users. Microsoft has invested significant resources to build robust defenses to stop malicious messages. In particular, Microsoft has engineered Office 365 to protect against spam, viruses and malware from even reaching Office 365 users. For example, Microsoft has built multiple spam filters into Office 365 mail accounts so customers' email addresses are protected from the moment the first message is received. Microsoft also uses three anti-malware engines to detect potentially dangerous software that may be sent to users. As part of this effort, Microsoft has also spent significant time and resources to flag millions of URLs as dangerous in order to stop threatening emails from reaching users.

21. Microsoft also offers Office 365 Advanced Threat Protection, which helps protect a user's mailbox against new, sophisticated attacks in real time. One protection included in this program, Safe Attachments, is a real-time behavioral malware analysis that uses machine learning techniques to evaluate email content for suspicious activity. Attachments deemed unsafe are sandboxed in a detonation chamber before being sent to recipients. Another program, Safe Links, protects Office 365 users clicking on a link in an

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

email. While the content is being scanned, the URLs are rewritten to go through Office 365. The URLs are examined in real time, at the time a user clicks them. If a link is unsafe, the user is warned not to visit the site or informed that the site has been blocked.

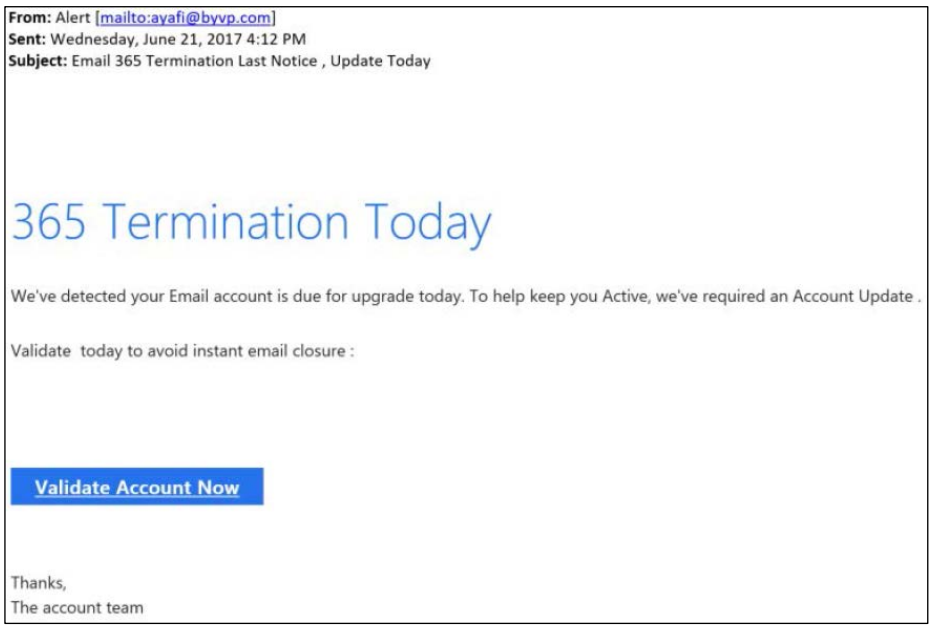
22. In addition to stopping phishing attempts before they reach users, Microsoft also investigates, identifies and stops the criminals behind malicious attacks. One of many ways Microsoft does this is by taking legal action, such as this one, to protect their customers from malicious attacks.

D. Defendants' Phishing Scheme

23. On information and belief, Defendants are engaged in a systematic and wide-spread phishing campaign perpetrated on unwitting people across the United States. Defendants' unlawful phishing scheme infringes Microsoft's intellectual property and misleads people into believing the messages are either from Microsoft or that Defendants are affiliated with Microsoft.

24. On information and belief, Defendants scheme starts by sending unsolicited bulk email purporting to be from the "The account team," to their potential victims ("Phishing Email"). The emails' subject is "Email 365 Termination Last Notice, Update Today." The body of the email states that "we've detected your Email account is due for upgrade today. To help keep you Active, we've required an Account Update." The email goes on to state "Validate today to avoid instant email closure" and then provides a button for the user to click on. A screenshot of this Phishing Email is below:

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax



From: Alert [mailto:ayafi@byvp.com]
Sent: Wednesday, June 21, 2017 4:12 PM
Subject: Email 365 Termination Last Notice , Update Today

365 Termination Today

We've detected your Email account is due for upgrade today. To help keep you Active, we've required an Account Update .

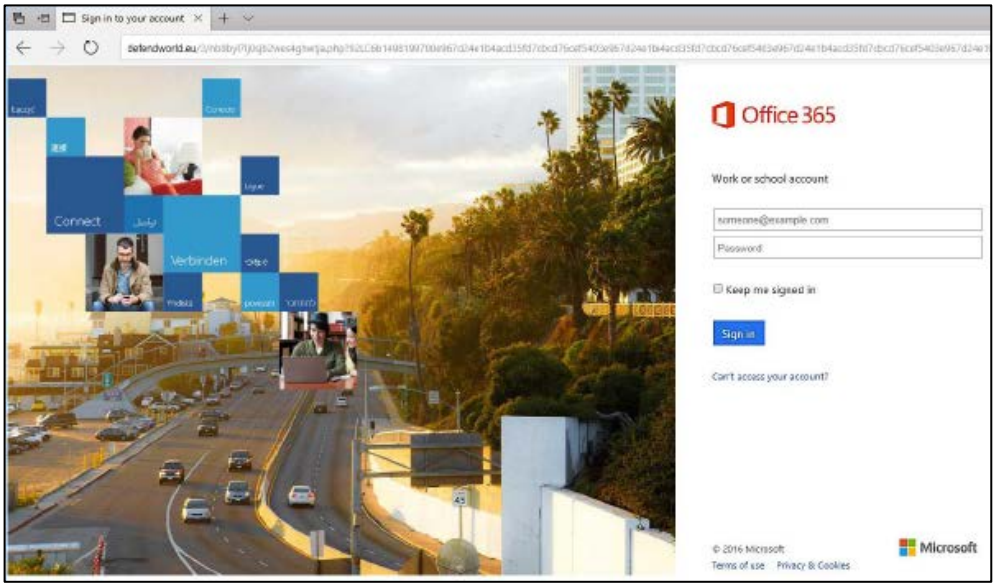
Validate today to avoid instant email closure :

Validate Account Now

Thanks,
The account team

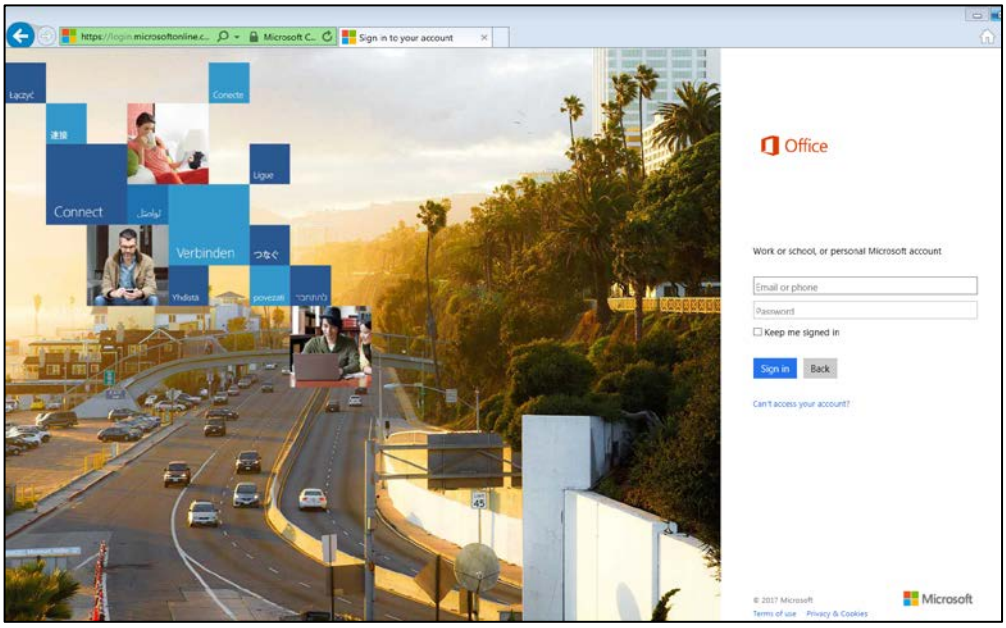
25. By clicking on the "Validate Account Now" button, the user is brought to a page that purports to be a login page to Office 365 (the "Phishing Page"). This page uses Microsoft's trademarks to create the appearance of being a legitimate Microsoft webpage when in reality it is a counterfeit of Microsoft's Office 365 login page that deceives consumers. The following are screenshots of Defendants' Phishing Page and Microsoft's authentic login page.

Defendants' Phishing Page:



Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

Microsoft's legitimate login page:



26. The Phishing Page to which the Phishing Email directed the recipient is not affiliated with Microsoft. The Phishing Page unlawfully uses Microsoft's valuable intellectual property for the purposes of deceiving visitors to the page into thinking it is a legitimate, authorized webpage from Microsoft and, on information and belief, does in fact, deceive some number of those visitors.

27. On information and belief, the Phishing Page was designed, maintained and operated by Defendants in a scheme to illegally capture Microsoft's customers' credentials (among other harm) and use those credentials to access the customers' Microsoft Account without authorization to further Defendants' unlawful scheme.

28. The Phishing Page is located on a website that uses the domain name defendworld.eu. Based on a search of public records relating to this domain, the registrar is GoDaddy.com, LLC. The registrant of the domain is listed as "Nuno Pires." The content from the website is hosted on a server that belongs to a third-party web hosting company, A2 Hosting, Inc.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

29. After entering login credentials on the Phishing Page, sometimes a Pop-Up dialogue box would present to the user ("Pop-Up"). This Pop-Up purported to be a safety alert from Microsoft: "Windows Defender Alert: Zeus Virus Detected In Your Computer." (The Zeus virus is a well-known Trojan horse malware program.) The Pop-Up provided a number for the user to call at "Microsoft's Technical Department." A screenshot of one version of the Pop-Up is below:

30. The Pop-Up is not affiliated with Microsoft, and unlawfully uses Microsoft's valuable intellectual property for the purposes of deceiving recipients into thinking it is a legitimate, authorized message from Microsoft.

31. On information and belief, the Pop-Up was designed, maintained and operated by Defendants in a scheme to unlawfully gain access to Office 365 accounts, a user's computer or system, Microsoft's computer or system or gain unauthorized access to other sensitive information. More specifically, the Pop-Up is part of a fraudulent technical support scam, whereby Defendants scare recipients into believing their Microsoft software is infected with a malicious virus in order to sell the victim unnecessary and phony "repair" services (among other potential harms).

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

32. The Pop-Up is hosted on a website that uses the domain azure1.us. Based on a search of public records relating to this domain, the registrar is NameCheap, Inc. The registrant of the domain is listed as "Anatoliu Golovin," and the registrant's email address is listed as opel73rus@gmail.com. The domain azure1.us is hosted on a server owned or controlled by Cloudflare, Inc.

VI. CAUSES OF ACTION

FIRST CLAIM

Violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030)

33. Plaintiff re-alleges each paragraph above as if fully set forth here.

34. On information and belief, Defendants knowingly and with intent to defraud, and in furtherance of their intended fraud, accessed and are accessing Microsoft's computer systems (a protected computer) without authorization, or in excess of any authorized access, and are thereby obtaining information (and other value) from Microsoft's computer systems and causing other damage to Microsoft and its customers.

35. On information and belief, Defendants knowingly and with intent to defraud obtained control of passwords or similar information through which Microsoft's computer systems computer may be accessed without authorization, with the intent to transfer the passwords or similar information to another person.

36. Microsoft's computer systems are used in and affect foreign and/or interstate commerce. Defendants' trafficking in passwords and other similar information affects interstate and/or foreign commerce.

37. On information and belief, as a result of the actions alleged above, Microsoft has suffered at least $5,000 in losses in a one year period, including but not limited to the loss of customer goodwill and harm to Microsoft's reputation as a result of Defendants' activities, the costs of identifying, assessing, and responding to those activities, including the costs of investigation and litigation, and the costs of remedying and/or restoring harm caused by Defendants' activities.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

38. As a result of the activities alleged above, Microsoft is entitled to recover its economic damages, including without limitation the damages and losses set forth above.

39. Microsoft has suffered, is suffering, and will continue to suffer irreparable harm unless Defendants are enjoined from further unlawful conduct. Microsoft has no adequate remedy at law for Defendants' wrongful conduct.

SECOND CLAIM

Violations of Washington's Consumer Electronic Mail Act (RCW 19.190.080)

40. Plaintiff re-alleges each paragraph above as if fully set forth here.

41. Microsoft owns and has duly and properly registered a number of trademarks in the United States Patent and Trademark Office on the Principal Register, as described in this Complaint.

42. On information and belief, through their illegal phishing pattern and practice, Defendants solicited, requested and took action to induce persons to provide personally identifying information by means of a web page, electronic mail message and the internet.

43. On information and belief, in designing, sending, maintaining and operating the Phishing Email, Phishing Page and Pop-Up, all of which illegally used Microsoft's intellectual property, including its trademarks, Defendant unlawfully represented themselves, either directly or by implication, to be with or affiliated with Microsoft— all without Microsoft's authority or approval.

44. As a result of Defendants' unlawful conduct, Microsoft is entitled to its actual damages or statutory damages of $5,000 per violation. Microsoft is also entitled to a trebling of any damages award because Defendants' phishing scheme constitutes a pattern and practice that violates RCW 19.190.080, and to its reasonable attorneys' fees and costs in bringing this case.

45. Microsoft has suffered, is suffering, and will continue to suffer irreparable harm unless Defendants are enjoined from further unlawful conduct. Microsoft has no adequate remedy at law for Defendants' wrongful conduct.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

THIRD CLAIM

Trademark Infringement (15 U.S.C. § 1114)

46. Plaintiff re-alleges each paragraph above as if fully set forth here.

47. Defendants' activities constitute infringement of Microsoft's federally registered trademarks and service marks with the registration numbers listed above.

48. Microsoft advertises, markets, distributes, and licenses its software and related components under the trademarks and service marks described above and uses these trademarks and service marks to distinguish Microsoft's products from the software and related items of others in the same or related fields.

49. Because of Microsoft's long, continuous, and exclusive use of these trademarks and service marks, they have come to mean, and are understood by customers, end users, and the public to signify software programs and related components or services of Microsoft.

50. The infringing materials that Defendants created, sent and continue to send to persons are likely to cause confusion, mistake, or deception as to the material's source, origin, or authenticity.

51. Further, Defendants' activities are likely to lead the public to conclude, incorrectly, that the infringing materials that Defendants send to persons originate with or are authorized by Microsoft, thereby harming Microsoft, its licensees, and the public.

52. As a result of Defendants' wrongful conduct, Microsoft is entitled to recover its actual damages, Defendants' profits attributable to the infringement, and treble damages and attorney fees pursuant to 15 U.S.C. § 1117 (a) and (b). Alternatively, Microsoft is entitled to statutory damages under 15 U.S.C. § 1117(c).

53. Microsoft is further entitled to injunctive relief and an order compelling the impounding of all infringing materials. Microsoft has no adequate remedy at law for Defendants' wrongful conduct because, among other things: (a) Microsoft's trademarks and service marks are unique and valuable property that have no readily determinable market value; (b) Defendants' infringement constitutes harm to Microsoft's reputation and goodwill such that

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

Microsoft could not be made whole by any monetary award; (c) if Defendants' wrongful conduct is allowed to continue, the public is likely to become further confused, mistaken, or deceived as to the source, origin or authenticity of the infringing materials; and (d) Defendants' wrongful conduct, and the resulting harm to Microsoft, is continuing.

FOURTH CLAIM

False Designation of Origin (15 U.S.C. § 1125(a))

54. Plaintiff re-alleges each paragraph above as if fully set forth here.

55. Microsoft advertises, markets, distributes, and licenses its software and services, and uses its trademarks and service marks outlined in this Complaint to distinguish Microsoft's software and related components and services from the products or services of others in the same field or related fields.

56. Microsoft has also designed non-functional distinctive and aesthetically pleasing displays, logos, icons, and graphic images for its software programs and related components. Microsoft's Office 365 login page contains a clearly articulable design and combination of elements, as shown in this Complaint, which uses Microsoft's name, certain trademarks, an image on the Pacific Coast Highway with blue tiles in the foreground on the left-hand side of the site, and a white login area on the right hand side ("Trade Dress").

57. Because of Microsoft's long, continuous, and exclusive use of the Microsoft marks, and because of its use of the Trade Dress, they are inherently distinctive or have come to mean, and are understood by customers, end users and the public to signify products and services of Microsoft.

58. On information and belief, Defendants' wrongful conduct includes the use of Microsoft's trademarks and service marks, Trade Dress, name, and/or imitation visual designs (specifically displays, logos, icons, and/or graphic designs virtually indistinguishable from Microsoft virtual designs) in connection with their goods and services, including on the Phishing Page and Pop-Up.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

59. On information and belief, Defendants engaged in such wrongful conduct with the purpose of misleading or confusing customers and the public as to the origin, authenticity, or association of the goods and services advertised, marketed, installed, provided, offered, or distributed in connection with Microsoft's trademarks, service marks, name, and imitation visual designs, and of trading on Microsoft's goodwill and business reputation. Defendants' conduct constitutes false designation of origin in violation of Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a).

60. As a result of Defendants' wrongful conduct, Microsoft is entitled to recover its actual damages, Defendants' profits, and treble damages and attorney fees pursuant to 15 U.S.C. § 1117.

61. Further, Microsoft is entitled to injunctive relief. Microsoft has no adequate remedy at law for Defendants' wrongful conduct because, among other things: (a) Microsoft's trademarks, service marks, Trade Dress, name, and visual designs are unique and valuable property which have no readily-determinable market value; (b) Defendants' advertising, marketing, or distribution of imitation visual designs constitutes harm to Microsoft such that Microsoft could not be made whole by any monetary award; and (c) Defendants' wrongful conduct, and the resulting damage to Microsoft, is continuing.

VII. PRAYER FOR RELIEF

WHEREFORE, Microsoft respectfully prays for the following relief:

A. That the Court enter judgment in Microsoft's favor on all claims;

B. That the Court permanently restrain and enjoin Defendants, their directors, principals, officers, agents, representatives, employees, attorneys, successors and assigns, and all others in active concert or participation with it, from:

i. Accessing, or attempting to access, Microsoft's computer systems without authorization, or in excess of any authorized access, and thereby obtaining information (and other value) from Microsoft's computer systems and causing other damage to Microsoft's computer systems and/or customers.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

ii. Any infringing use of, or making or inducing others to infringe, Microsoft's trademarks, service marks, or trade dress including the trademarks and trade dress identified above;

iii. Sending any commercial electronic messages that contain any of Microsoft's trademarks, service marks or trade dress, including those identified above, or otherwise representing that Defendants, either directly or by implication, are from or affiliated with Microsoft; and

iv. Assisting, aiding, or abetting any other person or business entity in engaging in or performing any of the activities listed above;

C. That Defendants be required to pay all general, special, actual, punitive and statutory damages which Microsoft has sustained, or will sustain, as a consequence of Defendants' unlawful acts, and that such damages be enhanced, doubled, or trebled as provided for by 15 U.S.C. § 1117(b) and RCW 19.190.090;

D. That Defendants be required to pay to Microsoft both the costs of this action and the reasonable attorneys' fees incurred by Microsoft in prosecuting this action, as provided for by 15 U.S.C. § 1117 and RCW 19.190.090 (among other places); and

E. That the Court grant Microsoft such other, further, and additional relief as the Court deems just and equitable.

DATED this 15th day of December, 2017.

DAVIS WRIGHT TREMAINE LLP
Attorneys for Microsoft Corporation

By *s/ Bonnie E. MacNaughton*
Bonnie E. MacNaughton, WSBA #36110

s/ James Harlan Wendell
James H. Wendell, WSBA #46489
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
Tel: (206) 622-3150
Fax: (206) 757-7700
Email: bonniemacnaughton@dwt.com
jamiewendell@dwt.com

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax